AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for enabling a network of database systems to provably track a message, wherein the message is created at an origin system and is destined to a recipient system, wherein the message passes through a first database system and a second database system, and wherein the origin system, the recipient system, the first database system, and the second database system are different from one another ~~to prove that an origin system sent a message~~, comprising:

determining a first digest of the message at the first database system;

~~receiving~~ sending ~~the message and a signed~~ the first digest ~~of the message~~ from the first database system to ~~at a~~ the second database system ~~from the origin system, wherein the signed first digest was created by signing a digest of the message using an origin private encryption key~~;

signing the first digest at the second database system using a ~~an origin public~~ second private encryption key that is associated with the second database system; ~~origin private encryption key to verify that the signed first digest was signed by the origin system, thereby proving that the origin system created and sent the message; and~~

sending the signed first digest from the second database system to the first database system;

validating the signed first digest at the first database system using a second public encryption key that is associated with the second private encryption key; and

if the signed first digest is valid, persistently storing the signed first digest at the first database system, thereby enabling the first database system to prove that the second database system requested to receive the message.

~~persistently storing the signed first digest with the message, which enables the database system to present the signed first digest as proof that the origin system sent the message, thereby preventing the sender from persuasively denying that the sender sent the message.~~

2. (Canceled).

3. (Canceled).

4. (Canceled).

5. (Currently amended) The method of claim 1, wherein the ~~origin~~ second public encryption key and the ~~origin~~ second private encryption key are a key pair of a public key encryption system.

6. (Canceled).

7. (Currently amended) The method of claim 1, wherein ~~computing~~ determining the first digest ~~includes~~ involves using one of message digest 2 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

8. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for enabling a network of database systems to ~~prove that an origin system~~

~~sent a message~~provably track a message, wherein the message is created at an origin system and is destined to a recipient system, wherein the message passes through a first database system and a second database system, and wherein the origin system, the recipient system, the first database system, and the second database system are different from one another, the method comprising:

determining a first digest of the message at the first database system;

~~receiving~~ sending ~~the message and a signed~~the first digest ~~of the message at a~~from the first database system to the second database system ~~from the origin system, wherein the signed first digest was created by signing a digest of the message using an origin private encryption key~~;

signing the first digest at the second database system using a~~n origin public~~ second private encryption key that is associated with the second database system;~~origin private encryption key to verify that the signed first digest was signed by the origin system, thereby proving that the origin system created and sent the message; and~~

sending the signed first digest from the second database system to the first database system;

validating the signed first digest at the first database system using a second public encryption key that is associated with the second private encryption key; and

if the signed first digest is valid, persistently storing the signed first digest at the first database system, thereby enabling the first database system to prove that the second database system requested to receive the message.

~~persistently storing the signed first digest with the message, which enables the database system to present the signed first digest as proof that the origin system sent the message, thereby preventing the sender from persuasively denying that the sender sent the message.~~

9. (Canceled).

10. (Canceled).

11. (Canceled).

12. (Currently amended) The computer-readable storage medium of claim 8, wherein the ~~origin~~ second public encryption key and the ~~origin~~ second private encryption key are a key pair of a public key encryption system.

13. (Canceled).

14. (Currently amended) The computer-readable storage medium of claim 8, wherein ~~computing~~ determining the first digest ~~includes~~ involves using one of message digest 2 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

15. (Currently amended) An apparatus for enabling a network of database systems to provably track a message, wherein the message is created at an origin system and is destined to a recipient system, wherein the message passes through a first database system and a second database system, and wherein the origin system, the recipient system, the first database system, and the second database system are different from one another ~~to prove that an origin system sent a message~~, comprising:

a determining mechanism that is configured to determine a first digest of the message at the first database system;

a first ~~receiving~~ sending mechanism that is configured to ~~receive~~ send the ~~message and a signed~~ first digest ~~of the message at a~~ from the first database

system to the second database system ~~from the origin system, wherein the signed first digest was created by signing a digest of the message using an origin private encryption key~~;

a signing~~a first verifying~~ mechanism that is configured to use a~~n origin public~~ second private encryption key that is associated with the second database system;~~origin private encryption key to verify that the signed first digest was signed by the origin system, thereby proving that the origin system created and sent the message; and~~

a second sending mechanism that is configured to send the signed first digest from the second database system to the first database system;

a validating mechanism that is configured to validate the signed first digest at the first database system using a second public encryption key that is associated with the second private encryption key; and

a storing mechanism, wherein if the signed first digest is valid, the storing mechanism is configured to persistently store the signed first digest at the first database system, thereby enabling the first database system to prove that the second database system requested to receive the message.

~~a first storing mechanism that is configured to persistently store the signed first digest with the message, which enables the database system to present the signed first digest as proof that the origin system sent the message, thereby preventing the sender from persuasively denying that the sender sent the message.~~

16. (Canceled).

17. (Canceled).

18. (Canceled).

19. (Currently amended) The apparatus of claim 15, wherein the ~~origin~~ second public encryption key and the ~~origin~~ second private encryption key are a key pair of a public key encryption system.

20. (Canceled).

21. (Currently amended) The apparatus of claim 15, wherein ~~computing~~ determining the first digest ~~includes~~ involves using one of message digest 2 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

22. (Canceled).

23. (Canceled).

24. (Canceled).